Carnegie Mellon
Software Engineering Institute

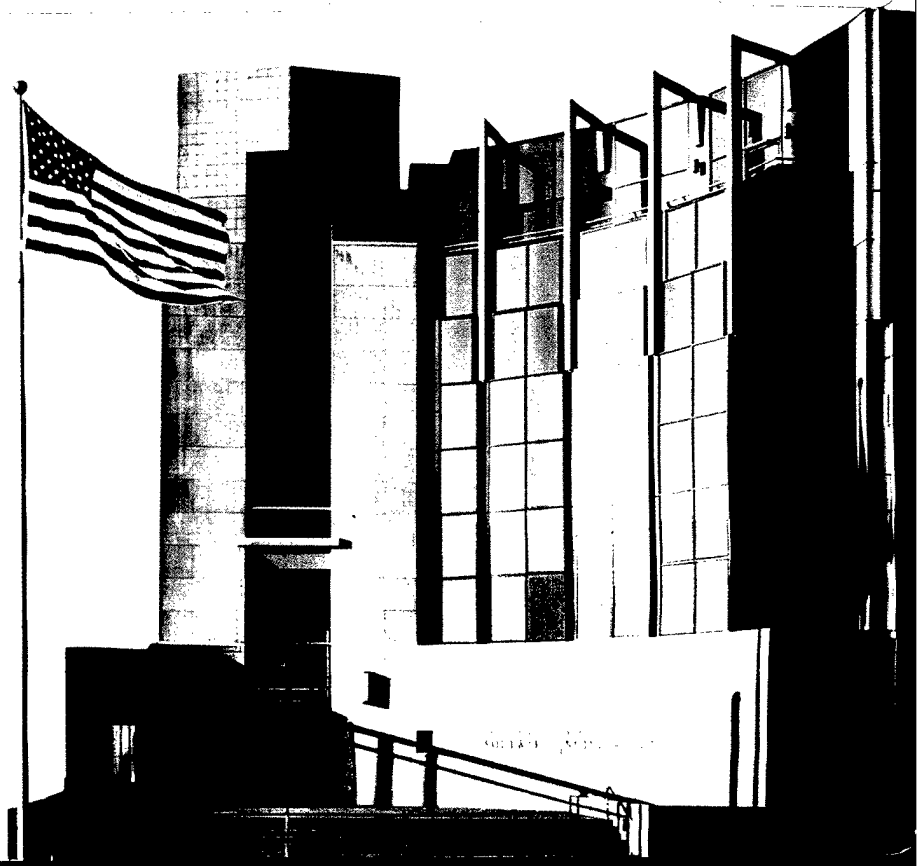
Information Assurance Curriculum and Certification: State of the Practice

Barbara S. Laswell, PhD
Derek Simmel
Sandra G. Behrens, PhD

July 1999

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

TECHNICAL REPORT
CMU/SEI-99-TR-021
ESC-TR-99-021



Carnegie Mellon University does not discriminate and Carnegie Mellon University is required not to discriminate in admission, employment, or administration of its programs or activities on the basis of race, color, national origin, sex or handicap in violation of Title VI of the Civil Rights Act of 1964, Title IX of the Educational Amendments of 1972 and Section 504 of the Rehabilitation Act of 1973 or other federal, state, or local laws or executive orders.

In addition, Carnegie Mellon University does not discriminate in admission, employment or administration of its programs on the basis of religion, creed, ancestry, belief, age, veteran status, sexual orientation or in violation of federal, state, or local laws or executive orders. However, in the judgment of the Carnegie Mellon Human Relations Commission, the Department of Defense policy of "Don't ask, don't tell, don't pursue" excludes openly gay, lesbian and bisexual students from receiving ROTC scholarships or serving in the military. Nevertheless, all ROTC classes at Carnegie Mellon University are available to all students.

Inquiries concerning application of these statements should be directed to the Provost, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-6684 or the Vice President for Enrollment, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-2056.

Obtain general information about Carnegie Mellon University by calling (412) 268-2000.

Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

Information Assurance Curriculum and Certification: State of the Practice

CMU/SEI-99-TR-021
ESC-TR-99-021

Barbara S. Laswell, PhD
Derek Simmel
Sandra G. Behrens, PhD

July 1999

Networked Systems Survivability Program

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Norton L. Compton, Lt Col., USAF
SEI Joint Program Office

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Tables

Abstract

The purpose of this document is to describe the state of the practice in information assurance and security curriculum and certification. The scope is not exhaustive, but rather illustrative of the types of activity occurring today within various organizations, including government, universities and research centers, professional societies, and the business community. Although individual courses are available, there apparently is no systematic agreement on the knowledge, skills, and abilities required to formulate a curriculum for information security professionals that enjoys broad-based support across organizations. As a result of Presidential Decision Directive 63 and the charge to protect the nation's critical infrastructures, the pressure is increasing to provide some minimum level of competence for system and network administrators working in the field of information assurance. Presently, several professional organizations offer certified professional designations.

What is needed is a comprehensive framework for curriculum and certification in information assurance and security. Currently the thrust for training focuses primarily on the technologies of information infrastructures. However, long-term solutions for the protection of critical information assets will require a more comprehensive approach in which senior executives and managers, as well as technical staff, develop strong and diverse skills that allow them to advance an organization's mission in a dynamic and increasingly hostile networked environment.

1 Overview of the Current Situation

1.1 Background

With the complexity of today's software, hardware, and networking products, it is difficult to properly configure systems and networks to use the strongest security measures appropriate to an organization's needs, even for people with good technical skills and training. Small mistakes can leave systems vulnerable and put information assets suddenly at risk. Long-term solutions for the protection of critical information assets will require fundamental changes in the architecture of computer systems as well as changes in the way technology is developed, deployed, and sustained. System and network operators need strong and diverse skills that allow them to work successfully in a dynamic and increasingly hostile networked environment.

1.2 The Problem

Currently, training for system and network administrators, their managers, and users insufficiently addresses requisite knowledge, skills, and abilities. While there are hundreds of training courses available, there is no clear and systematic path for identifying the kind of training that will result in the right learning in relation to a particular job or set of job task requirements. Additionally, the technology changes rapidly, resulting in the need for continued updating of skills. Consequently, course content is dynamic as well. Thus, any systematic effort to train and certify system and network administrators must account for changing technical requirements and course content. Even more problematic is the lack of a comprehensive body of knowledge that can be used to develop information assurance and security[1] curricula and to define the competencies and requirements for a workforce.

Furthermore, if the goal is to improve the security posture of U.S. critical infrastructures, then providing training to information technology security specialists and professionals addresses only the technical portion of the problem. Senior management must provide to those technical staff responsible for the secure administration of networked systems a clear sense of priority levels and appropriate policies, as well as risk-mitigation strategies, for securing various information assets. First-line managers of technical staff must be able to articulate the technical implications of these decisions so that cost-benefit tradeoffs can be evaluated. Thus, long-term solutions for the protection of critical information assets will require that senior executives and managers, as well as technical staff, develop strong and diverse skills.

1.3 Current Approaches

The U.S. government has started to address the information assurance problem for the federal sector by suggesting a federal government-wide strategy, as evidenced in Presidential Decision Directive 63 (PDD 63) . A possible approach to the information assurance curriculum and certification portion of the problem could utilize the *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, described in the NIST SP 800-16 document [Wilson 98]. This document outlines an information technology security body of knowledge, topics, and concepts. It could also provide a framework that could be used as the basis for a collaborative cross-agency effort. Also, areas within the Department of Defense are addressing the need to train information security specialists and to provide a career path for these professionals.

Clearly, the need exists for a comprehensive curriculum in information assurance and security, and for a systematic, efficient solution to the problem for both the private and public sectors.

One traditional approach to solving this problem is to identify training and educational institutions that provide courses on topics described in the NIST SP 800-16. A course-certifying body might evaluate the appropriateness of courses or course-module content and provide efficient methods of course delivery and learning evaluation (e.g., tests of knowledge for material covered in courses as they relate to job-specific security practices). In addition, evaluation criteria should be established so that training and education actually result in measurable improvements in security practices for all staff.

Another traditional approach is a program of professional certification, usually developed and administered by a professional association (such as the Information Systems Audit and Control Association). Currently, two kinds of certification exist in the field of information security: a broad-based, job-independent examination, such as the Certified Information System Security Professional (CISSIP) exam, and platform, tool, and technology-specific exams, such as those provided by Microsoft.

1.4 The Gap

Both traditional approaches currently exist, yet together they are insufficient to address the urgent and complex learning requirements engendered by the problem. What is needed is a way to ensure that knowledge, skills, and abilities are specifically and appropriately developed so that, over time, information assets are appropriately and effectively protected [Proceedings 98].

1.5 Proposed Framework

Knowledge and skills can be mastered in many ways. What the newly emerging field of information assurance and security lacks are two key elements.

First, a body of knowledge, specific to job tasks and responsibilities at all levels, should be described. Because the problem of information asset protection is growing and changing, some information that is now current will change or degrade over time. For example, it is important to understand how to configure and protect mail servers, domain name servers, and Web servers. However, the tools and practices required to accomplish this will change as the technologies and threats change. Another example involves the ways in which senior managers understand, evaluate, and mitigate exposure and threats to key assets as e-commerce flourishes. Therefore, part of this description should be an approach to evaluating the currency of the defined body of knowledge, and updating important information when required.

Second, a broader approach to job-specific certification should be established. Certification activities must measure both the knowledge of key subject matter as well as the ability to apply that information to job tasks. Certification approaches usually differ by type of job responsibility. For example, senior managers should know about auditing, legal issues, managing security risk, policy development, and e-commerce. Their certification might entail successfully participating in an intensive seminar with management simulations that evaluate a person's ability to perform key management tasks. System and network administrator certification might require knowledge of concepts such as those described in NIST SP800-16, and could measure such knowledge with a certification examination based on performance criteria set forth in the body of knowledge. Administrators could also demonstrate competence in specific practices at a hands-on training laboratory. Changes in technologies, staffing requirements, and fundamental skill requirements for various jobs might further require a renewal of certification through continuing education and re-testing of practice competence at a hands-on training laboratory.

In order to secure the information assets for national critical infrastructures, a comprehensive approach to addressing the security training and education issue might include the following:

- a framework that provides a usable structure for the identification, specification, development, and description of an overarching "body of knowledge" for the field of information assurance and security
- knowledge requirements for various job categories, including information and practices that are likely to change over time (i.e., the appropriate "body of knowledge" that should be acquired by staff with differing responsibilities)
- curriculum tracks for all job categories to ensure that staff receive important, relevant, and timely information
- collaboration partnerships between job-testing experts and institutes involved in information assurance and security to develop an effective approach to performance-based evaluation for individual certification
- a mechanism or process for providing unique information to course developers and training organizations who will work with the federal government and private sector organizations to assist staff in acquiring the requisite knowledge, skills, and abilities

- simulation laboratories that can be used to both train and assess a person's ability to perform secure practices at several levels of job responsibility
- collaboration among academic institutions, the federal government, and the business community to advance information assurance and security education and research

Currently the focus of information assurance and security curricula is on technical areas. However, long-term solutions for the protection of critical information assets will require senior executives and managers as well as technical staff to develop strong and diverse skills that allow them to advance an organization's mission in a dynamic and increasingly hostile networked environment.

Section 2 of this document describes the current activity in information assurance and security curriculum and certification. The scope is not exhaustive, but rather illustrative of the types of activity occurring today within various organizations, including government, universities and research centers, professional societies, and the business community. Section 3 of this document focuses on current efforts to provide a certified professional designation for system administrators and general security practitioners.

2 Current Activity in Curriculum and Certification

Pockets of activity exist within the government, universities and research centers, professional societies, and the business community related to information assurance and security. This activity includes courses, conferences, and certification of individuals for technical products. However, there apparently is no systematic agreement on the knowledge, skills, and abilities required to formulate a curriculum for information assurance and security professionals that enjoys broad-based support across organizations. Several universities have research centers and undergraduate and graduate programs in information assurance and security and related areas. However, the majority of technical training activity occurs within the vendor community where the emphasis is on certifying system administrators for products.

2.1 Government Sector

As a result of Presidential Decision Directive 63 and the charge to protect the nation's critical infrastructures, the pressure is increasing to provide some minimum level of competence for system and network administrators working in the field of information assurance. The Critical Infrastructure Assurance Office (CIAO) designated the Department of Commerce as responsible for the Coordinating Committees for Personnel and Training and for Education and Awareness. The Informational Seminar on PDD 63, sponsored by the General Services Administration (GSA) and the CIO Council Security Committee, identified improving system administrators' skills as an important area for addressing the lack of security and technical knowledge that will emerge from PDD 63 vulnerability assessments. [2]

Many initiatives have emerged as attempts to address the problem. Representative efforts that illustrate the broad scope of federal government sector organizations involved in information assurance and security education and training include the National Infrastructure Protection Center, which has an initiative to provide to its members a forum for education and training on infrastructure vulnerabilities and protection measures.[3] The National Institute of Standards and Technology (NIST) has identified the requirements for computer security training for federal information-technology personnel, based on job functions [Wilson 98]. One of the National Security Agency's initiatives is the National INFOSEC Education & Training Program that has established the Information Assurance Courseware Evaluation Process. The process is intended to assess the degree to which the various institution, college, and university curricula satisfy the NSTISSI standards.[4] The Federal Information Systems Security Educators' Association (FISSEA) at its 1999 conference had presentations dealing with curriculum and certification issues.[5]

Various agencies provide information assurance and security curricula to their constituents. For example, the Defense Information Systems Agency (DISA) provides INFOSEC training for information system security officers and managers.[6] The SPAWAR INFOSEC Office has a series of recommended information systems security courses for Navy personnel.[7] The Defense Security Institute provides consolidated training within the Department of Defense (DoD) for security professionals working both within DoD and the DoD contractor community.[8]

2.2 Professional Organizations

Professional organizations are involved with setting standards and offering continuing education activities such as conferences and courses for their members.

The International Federation of Information Processing (IFIP) has issued a statement on information security assessment and certification as part of an effort to establish international certification standards for individuals assessing IT systems and the information security management of those systems.[9] IFIP held the First World Conference on Information Security Education in Stockholm in June 1999.[10]

The Information Systems Audit and Control Association (ISACA) provides the Certified Information Systems Auditor Program. The American Society of Industrial Security (ASIS) provides certification for general security management [see Sections 3.2 and 3.4]. USENIX System Administrator's Guild (SAGE) has a certification subcommittee currently studying certification for system administrators [see Section 3.5].

Some professional organizations such as the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) have relationships established with organizations that are involved with accreditation of higher-education computer science and engineering programs. However, accreditation does not get to the level of granularity that includes requirements for information security curricula.[11]

Other professional organizations are not currently involved with setting standards and focus on offering courses and conferences to their members as part of a continuing professional development effort. For example, the Information Systems Security Association (ISSA) provides continuing technical education forums and conferences, such as the Open Systems Security 99 and ISSA Annual Conference.[12]

Table 1 lists professional organizations involved in continuing professional education relevant to developing professional skills in the areas of information assurance and security. Table I also lists the organizations that are currently involved in certification or have initiatives to study the issue. More detail on the certification process offered by four of these organizations is provided in Section 3 of this document.

Organization	Membership Target Population	Certification of Individuals	Sponsors Activities
Association for Computing Machinery (ACM)	IT professionals; SIG–Security, Audit, Control	Currently studying	Yes
American Society for Industrial Security (ASIS)	Industrial security management professionals	Yes	Yes
Federal Information Systems Security Educators' Association (FISSEA)	Federal information systems security educators	Currently studying	Yes
Institute of Electrical and Electronics Engineers, Inc.–Computer Society (IEEE–CS)	Electrical and electronic engineers in IEEE–CS	Currently studying	Yes
International Federation for Information Processing (IFIP)	IT professionals	Currently studying	Yes
Information Systems Audit and Control Association (ISACA)	Audit, control, and security professionals	Yes	Yes
International Information Systems Security Certification Consortium $(ISC)^2$	Information security professionals	Yes	
Information Systems Security Association (ISSA)	Information security professionals		Yes
National Classification Management	Information/computer security professionals		Yes

Society			
National Security Institute	Security professionals		Yes
USENIX System Administrator's Guild (SAGE)	System administrators	Currently studying	Yes
SANS Institute	System and network security administrators		Yes

Table 1: Professional Organizations Involved in Professional Education and Certification

2.3 University and Research Centers

Several universities offer graduate and undergraduate programs in information assurance and security and related areas, and have research centers associated with them. The Center for Research in Information Assurance and Security (CERIAS) at Purdue University provides "innovation and leadership in technology for the protection of information and information resources, and in the development and enhancement of expertise in information assurance and security."[13] James Madison University (JMU) has the Center for Research in Information Systems Security Education.[14] JMU also sponsors the National Colloquium for Information Systems Security Education for professionals in business and industry, academia, and government.[15]

The Center for Secure Information Systems (CSIS) at George Mason University offers a Graduate Certificate Program in Information Systems Security and also sponsors workshops, tutorials, and conferences.[16] The University of California, Davis has the Computer Security Laboratory and is involved in technical research.[17] The Department of Computer Science at the University of Idaho offers an undergraduate degree in Computer Security and degrees in Network System Security and Trusted Systems at the master's and doctorate levels.[18]

The H. John Heinz III School of Public Policy and Management at Carnegie Mellon University offers a Certificate in Information Security Management and a Master of Information Systems for Public Policy and Management with a concentration in Information Security Management.[19] The CERT® Coordination Center* at Carnegie Mellon's Software Engineering Institute offers courses in incident response and information security.[20]

The Information Operations Department of the National Defense University provides instruction on information assurance and information operations for students in the National

* CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office.

War College and the Industrial College of the Armed Forces.[21] The Naval Postgraduate School operates the Center for INFOSEC Studies and Research.[22]

Table 2 lists some of the university and research centers conducting courses and research in information assurance that are most frequently referenced in Web site links relating to computer security.

Universities and Research Centers
Carnegie Mellon University, H. John Heinz III School of Public Policy and Management, CERT® Coordination Center
George Mason University, Center for Secure Information Systems
George Washington University, Cyberspace Policy Institute
Idaho State University
James Madison University, Center for Research in Information Systems Security Education
Lawrence Livermore National Laboratory, Computer Security Technology Center
Massachusetts Institute of Technology
National Defense University
Naval Postgraduate School, Center for INFOSEC Studies and Research
Princeton University, Secure Internet Programming Group
Purdue University, Center for Education and Research in Information Assurance and Security
University of California, Berkeley
University of California, Davis, Computer Security Laboratory
University of Idaho

Table 2: University and Research Centers Conducting Courses and Research in Information Assurance

2.4 Business Community

The majority of the technical training for system and network administrators and other professionals in information security occurs in the private sector and is provided by software vendors that certify individuals in their various products [Martinez 99]. Some vendors, such as Cisco Systems, have curriculum tracks that cluster technology specializations and provide certification designations, such as "Cisco Certified Network Professional" with a specialization in security.[23]

Table 3 lists some companies currently offering or involved in technical training that includes information security subject matter.

Company	Certification Offered in Specific Products
AXENT Technologies, Inc.	AXENT security product training
Cisco Systems	Cisco Certified Network Professional–Security Specialization
Check Point Software Technologies, Ltd.	Check Point Certified Security Administrator; Check Point Certified Security Engineer
Computer Security Institute	Information security seminars and on-site training
IBM Tivoli Systems Global Security Laboratory	Certified Solutions Expert–Firewall; Certified Consultant–Security Management
Internet Systems Security	ISS Certified Engineer
Learning Tree International	System and Network Security Certified Professional
McAfee Software (Network Associates)	McAfee Certified Anti-Virus Administrator
Microsoft	Microsoft Certified Professional + Internet
Mitretek	Information Security Engineer
Network Associates, Inc.	Certified Network Expert NetSpecialist

Open Group Security Training Alliance	Courses target CIOs, IT managers
Prosoft Training.com	Certified Internet Webmaster–Security Professional; Certified UNIX Administrator
Sequent	Sequent Certified System Administrator
Sun Microsystems, Inc.	Sun Certified System Administrator; Sun Certified Network Administrator
Symantec	Certified Norton AntiVirus Consultant
USWeb Learning, Inc.	HyCurve Security Specialist
XOR	Courses in UNIX System Administration and Cisco Router administration

Table 3: Companies Involved in Technical Training

3 Description of Certified Professional Designations

Four professional societies currently offer certification for system administrators or general security practitioners. $(ISC)^2$ offers the designation of Certified Information System Security Professional (CISSP). The Information Systems Audit and Control Association (ISACA) provides the Certified Information Systems Auditor (CISA) certification. The Institute for Certification of Computer Professionals (ICCP) offers the Certified Computing Professional credential for a number of subject areas including system security. The American Society of Industrial Security (ASIS) offers generalist certification in security management. USENIX System Administrator's Guild (SAGE) is examining the issue of certification for generalist knowledge of system administrators.

3.1 Certified Information System Security Professional (CISSP)

The Certified Information System Security Professional (CISSP) is a designation provided by $(ISC)^2$ to a person who has three years of work related to information systems security, performed as a practitioner, auditor, consultant, vendor, investigator, or instructor, and who has successfully passed an exam and supports a code of ethics. An eight-day review seminar for the exam is available. Exam topics include policy, standards, legal issues, risk management and business continuity planning, computer architecture and system security, access control, cryptography, physical security, operations security, application security, and communications security. Re-certification is granted every three years after an individual earns 120 continuing education credits, which can be earned through activities such as courses, conference attendance, publications, and service on professional security boards.[24] As of early 1998 1,500 individuals held the CISSP designation.[25]

3.2 Certified Information Systems Auditor (CISA)

The Information Systems Audit and Control Association (ISACA) provides the Certified Information Systems Auditor (CISA) certification to individuals with five years of experience in information systems audit, control, and security (some academic work may be substituted for experience), who successfully pass an exam, and who support a code of ethics. Review courses and reference materials are available. The exam is based on job analysis of tasks performed by information systems audit, control, and security professionals. Topics on information systems include audit standards and practices, organization/management, process, integrity/confidentiality/availability, and development/acquisition/maintenance. Re-certification is

granted every three years after a person earns 120 continuing education credits. In 1998 approximately 4,300 professionals took the exam and 54% passed.[26]

3.3 Certified Computing Professional (CCP)

The Institute for Certification of Computer Professionals offers the designation of Certified Computing Professional (CCP) to computer professionals who have four years of experience (or two years of experience plus a bachelor's degree in a related field) and pass a core exam and two specialty exams. The core examination covers general knowledge on information systems and technology. The specialty exam in information security includes testing on risk assessment, recovery, security, system design, and security management. Re-certification requires 120 hours of educational and professional activities. Currently about 50,000 people hold CCPs, some of whom may have taken the specialty exam in systems security.[27]

3.4 Certified Protection Professional (CPP)

The American Society of Industrial Security (ASIS) offers generalist certification as a Certified Protection Professional (CPP) in security management to individuals who have nine years of experience in general security management (this may include academic credits) and who successfully pass an exam. The items on the exam are based on a job analysis of the functions required for effective performance of security management. Topics include emergency management, investigations, legal aspects, personnel security, physical security, protection of sensitive information, and security management. The target membership of ASIS, a professional organization, is professionals responsible for security, including managers and directors of security, corporate executives, and other management personnel, as well as people in related areas such as attorneys, architects, and law enforcement officials. The ASIS Standing Committee on Computer Security targets general security managers and not system administrators. ASIS International has 30,000 members; 4,000 people currently hold the CPP designation.[28]

3.5 USENIX System Administrator's Guild (SAGE)

USENIX System Administrator's Guild (SAGE) is studying the issues of certification and continuing education. SAGE's efforts to establish standards of practice include a competency checklist, the purpose of which is to begin developing a taxonomy of system administration skills and competency domains of knowledge [Kuncicky 98]. The SAGE Certification Subcommittee currently has a project scheduled for completion by the end of 1999 to develop skill requirements and evaluate testing methodologies and implementation logistics. SAGE will then decide whether it will manage a certification program.[29]

The requirements of the four certification programs of $(ISC)^2$, ISACA, ICCP, and ASIS are compared in Table 4.

Certification Designation	Organization	Experience Required (years)	Code of Ethics	Exam	Review Courses	Re-certification (period; requirements)	Number Taking Exam in 1998	Number of Current Holders
CISSP	(ISC)^2	3	Yes	Yes	8-day review optional	Every 3 years; exam or 120 CEUs	N/A	1,500
CISA	ISACA	5*	Yes	Yes	Courses and materials available	3 years; 120 CEUs	4,300; 54% passed	N/A
CCP	ICCP	4*	Yes	Yes	Courses and materials available	3 years; 120 CEUs	N/A	50,000
CPP	ASIS	9*	Yes	Yes	Courses and materials available	3 years; 18 CEUs plus other	N/A	4,000

*Some academic work may be substituted for experience.

Table 4: Comparison of Certification Designations

4 Summary

There apparently is no systematic agreement on the knowledge, skills, and abilities required to formulate a comprehensive curriculum for information assurance and security that enjoys broad-based support across organizations. Presently, the majority of technical training activity occurs within the vendor community where the emphasis is on certifying system administrators for products. There also is no certification infrastructure in place that enjoys broad-based support across organizations. Several professional organizations currently have certification programs. Some involve only testing, while others also provide access to courses within a prescribed curriculum. In the academic community, a growing number of universities have undergraduate and graduate programs and research centers in information assurance and security. The federal government makes courses in information assurance and security available to its constituents.

What is needed is a comprehensive framework for curriculum and certification in information assurance and security that addresses the management challenges as well as the technical challenges of protecting the nation's critical infrastructures. Current activity focuses primarily on the technologies of information infrastructures. However, long-term solutions for the protection of critical information assets will require a more comprehensive approach in which senior executives and managers, as well as technical staffs, develop strong and diverse skills that allow them to advance an organization's mission in a dynamic and increasingly hostile networked environment.

Endnotes

[1] For definitions of "information assurance" and "information systems security" as used in this document, see *National Information Systems Security (INFOSEC) Glossary*, NSTISSI No. 4009, National Security Telecommunications and Information Systems Security Committee, August 1997, p.21.

[2] Mark Boster, "CIO Council Security Committee and PDD 63," Oct. 13, 1998, Washington, DC. http://www.ciao.gov/seminar19981013.html

[3] http://www.nipc.gov/nipc/nipc.htm

[4] http://www.nsa.gov:8080/isso/programs/nietp/corseval.htm

[5] The 1999 12th Annual FISSEA Conference, "Paradigm Shifts for Teaching Computer Security in the New Millennium," included two presentations specifically dealing with curriculum and certification issues. They were "Assembling a Curriulum for Various Security Disciplines," (Jane Powanda, Mitretek) and "Professionalization: Becoming a CISS" (Wayne Madsen, senior fellow, Electronic Privacy Information Center). http://csrc.nist.gov/organizations/fissea/99Fissea.html

[6] http://www.disa.mil/infosec/itfcour.html

[7] http://infosec.nosc.mil/TRAINING/training2.html

[8] http://www.dss.mil/training/

[9] http://www.ifip.tu-graz.ac.at/TC11/TC11.crypto/certification.html

[10] http://www.dsv.su.se/WISE1/index2.html

[11] The Computer Science Accreditation Board (CSAB) accredits post-secondary baccalaureate programs in computer science and the Accreditation Board for Engineering and Technology (ABET) accredits engineering technology programs for higher education through ABET. CSAB and ABET have made preliminary agreements to merge and to accredit software engineering programs.

[12] http://www.issa-intl.org/mis99.html

[13] http://www.cs.purdue.edu/coast/cerias/about.html

[14] http://www.infosec.jmu.edu

[15] http://www.infosec.jmu.edu/ncisse/

[16] http://www.isse.gmu.edu/~csis/index.html

[17] http://seclab.cs.ucdavis.edu/

[18] http://www.cs.uidaho.edu/

[19] http://www.cmu.edu

[20] http://www.cert.org

[21] http://www.ndu.edu/irmc/

[22] http://cisr.nps.navy.mil/

[23] http://www.cisco.com/warp/public/10/wwtraining/certprog/special/course.html

[24] http://www.isc2.org

[25] http://www.infosecnews.com/scmagazine/1998_04/lastword/lastword.html

[26] http://www.isaca.org

[27] http://www.iccp.org

[28] http://www.asisonline.org

[29] http://www.usenix.org/sage/cert/certification.html

References

[Kuncicky 98] Kuncicky, David and Bruce Alan Wynn. *Education and Training System Administrators: A Survey.* Berkeley, CA: The USENIX Association, 1998.

[Martinez 99] Martinez, Anne. *Get Certified & Get Ahead.* New York, NY: McGraw-Hill, 1999.

[Proceedings 98] "Proceedings of the Information Security Education Needs Workshop," unpublished. Arlington, VA: Software Engineering Institute, Carnegie Mellon University, September 1–2, 1998.

[Wilson 98] Wilson, Mark, ed. *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, NIST Special Publication 800-16, National Institute of Standards and Technology, U.S. Department of Commerce, 1998.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (LEAVE BLANK)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	July 1999	Technical Report, July 1999

3. TITLE AND SUBTITLE
Information Assurance Curriculum and Certification: State of the Practice

5. FUNDING NUMBERS
C — F19628-95-C-0003

6. AUTHOR(S)
Barbara S. Laswell, PhD
Derek Simmel
Sandra G. Behrens, PhD

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

7. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-99-TR-021
ESC-TR-99-021

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12.A DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12.B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

The purpose of this document is to describe the state of the practice in information assurance and security curriculum and certification. The scope is not exhaustive, but rather illustrative of the types of activity occurring today within various organizations, including government, universities and research centers, professional societies, and the business community. Although individual courses are available, there apparently is no systematic agreement on the knowledge, skills, and abilities required to formulate a curriculum for information security professionals that enjoys broad-based support across organizations. As a result of Presidential Decision Directive 63 and the charge to protect the nation's critical infrastructures, the pressure is increasing to provide some minimum level of competence for system and network administrators working in the field of information assurance. Presently, several professional organizations offer certified professional designations.

What is needed is a comprehensive framework for curriculum and certification in information assurance and security. Currently the thrust for training focuses primarily on the technologies of information infrastructures. However, long-term solutions for the protection of critical information assets will require a more comprehensive approach in which senior executives and managers, as well as technical staff, develop strong and diverse skills that allow them to advance an organization's mission in a dynamic and increasingly hostile networked environment.

14. SUBJECT TERMS

15. NUMBER OF PAGES
32

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL